Notice of Allowability	Application No.	Applicant(s)	
	09/651,901	JAKUBOWSKI ET AL.	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *3/10/2006*.

2. ☒ The allowed claim(s) is/are *1-7,9-11,13-23,25-29,31-34 and 36-44*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 2/10/06, 3/10/06
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Taghi T. Arani
Primary examiner
Aa 2131
Taghi T. Arani
4/7/06

DETAILED ACTION

1. The text of those sections of Title 35 U.S. Code not included in this section can be found in the prior office action.

2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.

3. Claims 8, 12, 24,30, and 35 have been cancelled.

4. Claims 1, 13, 16, 29, 34, 36, and 38 have been amended.

5. Claims 1-7, 9-11, 13-23, 25-29, 31-34, 36-44, now re-numbered as claims 1-39 are pending.

EXAMINER'S AMENDMENT

6. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Allan Sponseller on 04/10/2006.

Claims 8 and 24 have been canceled.

Claims 1, 13, 16, 29, 34, and 38 have been replaced with:

1. (Currently amended) One or more computer readable media having stored thereon a program that, when executed by one or more processors, causes the one or more processors to perform acts including:

identifying a plurality of key instructions in a function;

inserting into the function, for each of the plurality of key instructions, an extra instruction that modifies content of a register based at least in part on the corresponding key instruction;

identifying a set of inputs to the function, wherein the identifying a set of inputs comprises identifying a set of input patterns to the function that result in different valid computation paths in the function being taken; and

determining a checksum for the function based at least in part on modifications made to the content of the register by the extra instructions when the function is executed with the set of inputs.

13. (Currently amended) A method implemented at least in part by a computing device, the method comprising:

generating a checksum on bytes of a digital good based on modifications made by the digital good rather than on reading the bytes, wherein the generating comprises:

identifying a plurality of key instructions in a function;

inserting into the function, for each of the plurality of key instructions, an extra instruction that modifies a register based at least in part on the corresponding key instruction;

identifying a set of inputs to the function; and

determining a checksum for the function by mapping contents of the register to the set of inputs, wherein the determining comprises determining as the checksum both an initial value (x_0) and a calculated value (*Cks*), wherein the initial value is a first input of the set

of inputs, and wherein the calculated value is calculated according to the following process:

Start with $x = x_0$
Cks := $f(x_0)$ XOR x_0
For i=1 to K do
    $x_i := g(f(x_{i-1}))$
    Cks += $f(x_i)$ XOR x_i
End for

wherein *K* is the number of inputs in the set of inputs and *g* represents the mapping function.

14. (Currently amended) ~~A~~ The method as recited in claim 13, wherein the identifying comprises identifying, as a key instruction, each instruction in the function that possibly modifies a register or a flag.

16. (Currently amended) A method implemented at least in part by a computing device, the method comprising: method comprising:

inserting, into a segment of a digital good, a plurality of instructions that modify content of a register;

identifying a set of inputs to the segment, wherein the identifying a set of inputs comprises identifying a set of input patterns to the segment that result in different valid computation paths in the segment being taken; and

determining a checksum value for the segment based at least in part on modifications made to the content of the register by the plurality of instructions when the plurality of instructions are executed with the set of inputs to the segment.

17. (Currently amended) ~~A~~ The method as recited in claim 16, wherein the inserting comprises:

identifying a plurality of key instructions in the segment; and

inserting into the segment, for each of the plurality of key instructions, an extra instruction that modifies the content of a register based at least in part on the corresponding key instruction.

18. (Currently amended) ~~A~~ The method as recited in claim 17, wherein the identifying a plurality of key instructions comprises identifying, as a key instruction, each instruction in the segment that possibly modifies the content of a register or a flag.

19. (Currently) ~~A~~ The method as recited in claim 17, wherein the identifying a plurality of key instructions comprises identifying, as the plurality of key instructions, a plurality of instructions that each modify the content of one or more registers or one or more flags.

20. (Currently amended) ~~A~~ The method as recited in claim 16, wherein the inserting comprises inserting each of the plurality of instructions in a location within the segment so that the instruction is executed if a corresponding key instruction is executed.

21. (Currently amended) ~~A~~ The method as recited in claim 16, wherein the inserting comprises inserting each of the plurality of instructions in a location within the segment so that the instruction is executed after a corresponding key instruction is executed.

22. (Currently amended) ~~A~~ The method as recited in claim 16, wherein the inserting comprises inserting the extra instructions into the segment without altering a control flow of the segment.

23. (Currently amended) ~~A~~ The method as recited in claim 16, wherein the inserting comprises inserting a plurality of extra instructions that modify the content of one or more registers.

25. (Currently amended) ~~A~~ The method as recited in claim 16, wherein the identifying a set of inputs comprises identifying a set of input patterns to the segment that result in all valid computation paths in the segment being taken.

26. (Currently amended) ~~A~~ The method as recited in claim 16, wherein the determining comprises determining as the checksum value both an initial value (x_0) and a calculated value (*Cks*), wherein the initial value is a first input of the set of inputs, and wherein the calculated value is calculated according to the following process:

Start with $x = x_0$

Cks := $f(x_0)$ XOR x_0

For i=1 to K do

$x_i := g(f(x_{i-1}))$

Cks += $f(x_i)$ XOR x_i

End for

wherein *K* is the number of inputs in the set of inputs and *g* represents the mapping function.

27. (Currently amended) ~~A~~ The method as recited in claim 16, wherein the digital good comprises a software program.

29. (Currently amended) A production system, comprising:

a memory to store an original program; and

a production server equipped with an oblivious checking protection tool that is used to augment the original program for protection purposes, the production server being configured to identify a plurality of segments in the original program and apply oblivious checking to each of the plurality of segments by:

inserting, into the segment, a plurality of instructions that modify content of a register;

identifying a set of inputs to the segment, wherein the identifying a set of inputs comprises identifying a set of input patterns to the segment that result in different valid computation paths in the segment being taken; and

determining a checksum value for the segment based at least in part on modifications made to the content of the register by the plurality of instructions when the segment is executed with the set of inputs.

34. (Currently amended) A client-server system, comprising:

a production server to apply oblivious checking to a program to produce a protected program by:

inserting, into a segment of the program, a plurality of instructions that modify content of a register;

identifying a set of inputs to the segment; and

determining a checksum value for the segment based at least in part on modifications made to the content of the register by the plurality of instructions when the segment is executed with the set of inputs, wherein the determining comprises determining as the checksum both an

initial value (x_0) and a calculated value (*Cks*), wherein the initial value is a first input of the set of inputs, and wherein the calculated value is calculated according to the following process:

Start with $x = x_0$

Cks := $f(x_0)$ XOR x_0

For i=1 to K do

$x_i := g(f(x_{i-1}))$

Cks += $f(x_i)$ XOR x_i

End for

wherein *K* is the number of inputs in the set of inputs and *g* represents the mapping function; and a client to store and execute the protected program, the client being configured to evaluate the protected program to determine whether the protected program has been tampered with.

38. (Currently amended) One or more computer readable media having stored thereon a plurality of instructions that, when executed by one or more processors, causes the one or more processors to perform acts including:

generating a checksum value for a segment of a digital good based at least in part on both a set of inputs to the segment and the content of a register that results from applying the set of inputs to the segment and modification of the content of the register by instructions in the segment, wherein the set of inputs comprises a set of input patterns to the segment that result in different valid computation paths in the segment being taken;

comparing the generated checksum value to a stored checksum value corresponding to the segment; and

determining that the digital good has been tampered with if the generated checksum value does not match the stored checksum value.

42. (Currently) ~~A~~ The method as recited in claim 16, wherein the determining comprises determining the checksum value so that if the segment is changed the checksum value will also change.

44. (Currently amended) ~~A~~ The method as recited in claim 16, further comprising: executing the segment a plurality of times, each execution using a different input of the set of inputs.

Response to Arguments

7. Applicant's arguments filed 2/10/2006 (in view of the Examiner's Amendment) have been fully considered and they are persuasive.

Allowable Subject matter

8. Claims 1-7, 9-11, 13-23, 25-29, 31-34, 36-44 are allowed over prior art of record.

Conclusion

9. Prior arts made of record, not relied upon:

US 7,001,119 B1 to Jia et al. is directed to instruction /data protection employing derived obscuring instruction/data.

US 2001/0037450 to Metlitski et al. discloses system and method for process protection.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Taghi T. Arani, Ph.D.
Primary Examiner
Art Unit 2131
4/12/2006